

**REMARKS**

**I. STATUS OF THE CLAIMS**

Claims 1-15 and 18-20 are rejected under 35 U.S.C. § 103(a).

Claims 2, 13 and 19 are cancelled.

New claim 21 is added. Support for the new claim is found, for example, in Fig. 9 and page 16, line 33 through page 19, line 19, of the application.

Claim 1 is amended herein. Support for the amendments is found, for example, on page 8, lines 1-30, of the application.

Claims 1, 3-12, 14, 15, 18, 20 and 21 are currently pending.

**II. REJECTION OF CLAIMS 1-15 AND 18-20 UNDER 35 U.S.C. 103(a) AS BEING UNPATENTABLE OVER SREY ET AL. (U.S. PATENT NO. 6,141,436) IN VIEW OF BONGIORNO ET AL. (U.S. PATENT NO. 6,292,045) AND FURTHER IN VIEW OF SANO ET AL. (U.S. PATENT NO. 6,985,582)**

In the Examiner Interview conducted on August 20, 2007, the Examiner indicated that amendments clarifying the function of the lock system and/or how data is decoded may possibly distinguish over the art of record. The claims are amended herein to further clarify the operation of the lock release system. Amended claim 1 recites a time setting unit that enables a user of the data converter to change the period of time for the lock system in accordance with the user's operation environment. Amended claim 18 recites somewhat similar features. The Applicant respectfully submits that the cited art fails to teach these features.

Srey discusses that a user may press a predetermined number of keys to generate a lock or unlock code. See column 3, lines 29-36 of Srey. However, Srey is silent as to a user changing a period of time for a lock system in accordance with the user's operating environment. Such a feature allows a user, for instance, to increase the time of the lock system in a safe environment and decrease the time in an unsafe environment. Further, Bongiorno and Sano present no teaching or suggestion of modification of Srey to incorporate this feature.

Claim 1 also recites a data conversion unit configured to encrypt data originating in an external device and return the encrypted originated data back to the same external device to be stored therein. Claim 18 recites somewhat similar features. The Applicant respectfully submits that the cited art fails to teach these features.

The Office Action states on pages 3 and 4 that:

Sano in encryption/ decryption unit and storage medium teaches the conversion unit configured to encrypt the decrypt data and decrypt the encrypt data and

returns it back to the external device, and a connector part configured to directly connect to and disconnect from a slot part of the external device as insertably connects and disconnects, (see figure 1, numerical 10, the encryption and decryption unit, and numerical 21 and 22 as the data that needs to be encrypted or decrypted, and figure 12, the numerical 231 and the memory card the "external device", and for the description please see col. 4, lines 5-18, 35-40 and col. 14, lines 51-68) as claimed.

Sano discusses that "FIG. 12 is a block diagram showing an embodiment in which an encryption/decryption unit and storage medium of the present invention are implemented." See column 14, lines 51-53, of Sano. As illustrated in Fig. 12 and described in the associated description thereof in column 14, lines 51-68, Sano fails to disclose the above features of claim 1.

Per the above, the Office Action contends that the "memory card" designated by the numeral 231 in Fig. 12 of Sano discloses an "external device", as recited in claim 12. However, as stated in Sano, "a memory card 231 is **connected to** the system bus 233 through an expansion connector 229." Column 14, lines 62-64, of Sano. Sano discusses that the "storage medium" may be typical storage devices, such as a "magnetic disk, floppy disk, hard disk, optical disk (CD-ROM, CD-R, DVD, or the like), magneto-optical disk (MO or the like), and semiconductor memory." See column 15, lines 1-7, of Sano. From Fig. 12 and the associated description, it appears that the memory and other features are all included in one unit. In fact, it is likely that the device described in Sano would be inoperable without memory. As such, Sano fails to disclose an external device. Srey and Bongiorno also do not teach these features. Thus, the cited art, both individually and in combination, fails to disclose the above features of claim 1.

Claim 1 also recites a lock system configured to lock a data conversion function of said data conversion unit in a disabled state after a passage of a predetermined period of time so as to prevent said data conversion unit from encrypting and decrypting the data. Claim 18 recites somewhat similar features. The Office Action states that Srey "fails to disclose a predetermined period of time to prevent data conversion", but asserts that Bongiorno discloses this feature, citing column 1, lines 10-18 and 30-39, relating to microprocessor clocking. The Applicant respectfully submits that the cited art fails to teach the above feature.

The Office Action states on page 3 that:

Bongiorno teaches that cellular phones contains the microprocessors and that the microprocessors does include clocks "predetermined period of time" that while in operation does disable the operation once the predetermined time period happens.

The cited section of Bongiorno discusses that "the microprocessor chip contains a watchdog timer that prevents equipment faults or a computer program from looping endlessly or becoming

idle because of program errors." See column 1, lines 29-32, of Bongiorno. The watchdog timer generates and sends out "a signal to reset the microprocessor and to disable the microprocessor-based chip after a pre-set time-out period has elapsed during which the microprocessor-based chip has experienced such failure or system lockup." See column 1, lines 32-36, of Bongiorno. In other words, the microprocessor is disabled and reset after a predetermined time period passes because it is assumed that the microprocessor is stuck in an infinite loop.

Claim 1, on the other hand, recites disabling the data conversion unit after the passage of a predetermined period of time so as to prevent the data conversion unit from encrypting and decrypting the data. Presumably, the microprocessor discussed in Bongiorno becomes operable again after resetting. As such, Bongiorno does not teach disabling a data conversion unit in the manner recited in claim 1. In fact, because the microprocessor resets, Bongiorno teaches away from disabling a data conversion unit. Srey and Sano also fail to teach this feature. Thus, the cited art, both individually and in combination, fails to disclose the above features of claim 1.

Claim 1 further recites that the data converter includes a connector part configured to directly connect to and disconnect from a slot part of the external device, the data converter insertably connecting to and disconnecting from the external device so as to allow data exchange between the data converter and the external device. Claim 18 recites somewhat similar features. Per the above, the Office Action states on page 4 that Fig. 1, numerals 10, 21 and 22 and Fig. 12, numeral 231, column 4, lines 5-18, 35-40 and column 14, lines 51-68, of Sano disclose these features. The Applicant respectfully submits that the cited art fails to teach these features.

The Office Action contends that the "memory card" designated by the numeral 231 in Fig. 12 of Sano is an "external device", as recited in claim 12. Per the arguments above, a memory card is not an external device. Further, claim 1 recites that the **data converter** includes a connector part configured to insertably connect to and disconnect from the external device. As stated in Sano, "a **memory card** 231 is connected to the system bus 233 through an expansion connector 229." Column 14, lines 62-64, of Sano. As explicitly stated in Sano, the memory card is connected to the system bus of the encryption/decryption unit, not vice versa. As such, Sano fails to disclose a data converter that includes a connector part configured to directly connect to and disconnect from a slot part of the external device. Srey and Bongiorno also do not teach these features. Thus, the cited art, both individually and in combination, fails to disclose the above features of claim 1.

The above comments are specifically directed to claim 1. However, it is respectfully submitted that the comments would be helpful in understanding various differences of various other claims over the cited art.

In view of the above, it is respectfully submitted that the rejection is overcome.

### III. NEW CLAIM

New claim 21 is added herein. Claim 21 recites that after the predetermined period of time passes, the lock release system requests that the user enter security information, and if security information is not entered for a second predetermined period of time, the lock system locks the data conversion function of the data conversion unit in a disabled state. No teaching or suggestion of this feature is found in the cited art and claim 21 also distinguishes over the aforementioned references.

### IV. CONCLUSION

There being no further outstanding objections or rejections, it is submitted that the application is in condition for allowance. An early action to that effect is courteously solicited.

Finally, if there are any formal matters remaining after this response, the Examiner is requested to telephone the undersigned to attend to these matters.

If there are any additional fees associated with filing of this Amendment, please charge the same to our Deposit Account No. 19-3935.

Respectfully submitted,

STAAS & HALSEY LLP

Date: 9-21-07

By: MALE  
Michael A. Leonard II  
Registration No. 60,180

1201 New York Avenue, NW, 7th Floor  
Washington, D.C. 20005  
Telephone: (202) 434-1500  
Facsimile: (202) 434-1501